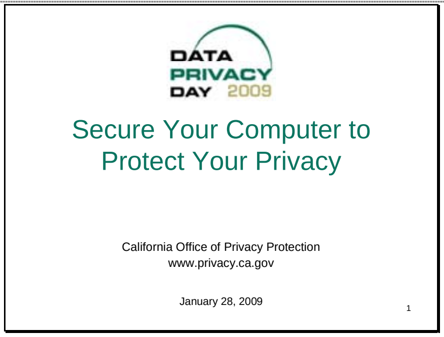
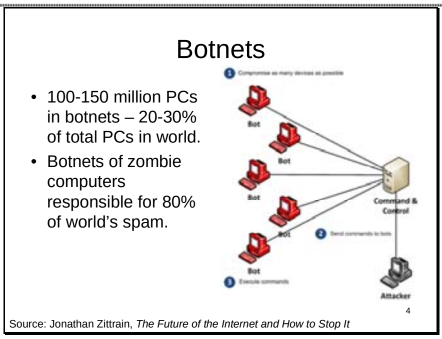
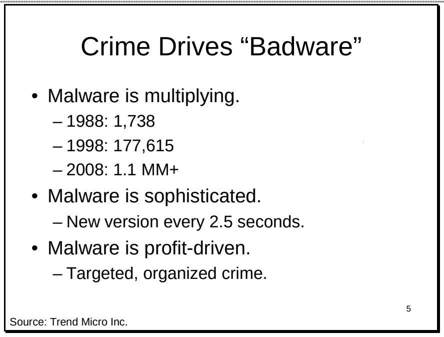
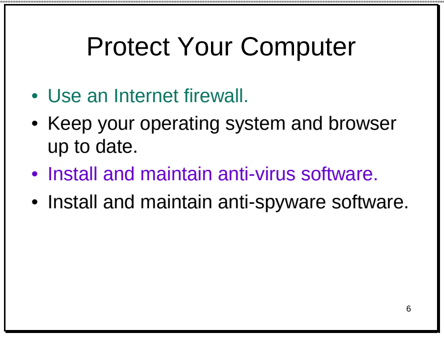
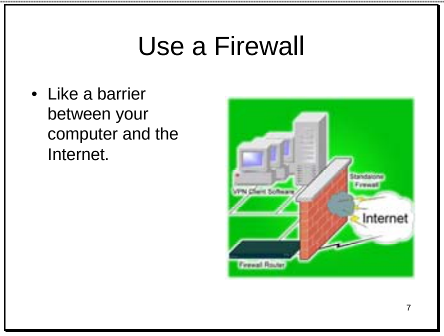
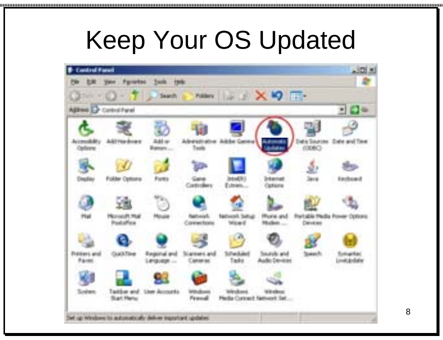
Secure Your Computer to Protect Your Privacy: Speaker Notes for Presentation

This presentation on securing home computers was developed by the California Office of Privacy Protection for use by community organizations and businesses to train individuals on securing their home computers. For more information on this topic, see *Consumer Information Sheet 12: Protect Your Computer from Viruses, Hackers and Spies* at www.privacy.ca.gov.

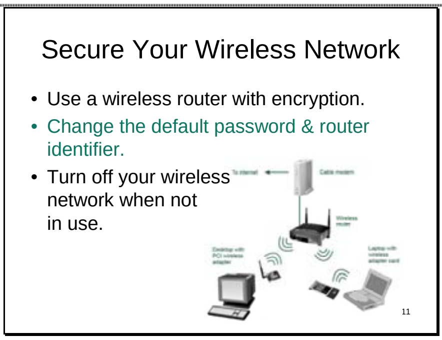
Slide 1	 DATA PRIVACY DAY 2009 Secure Your Computer to Protect Your Privacy California Office of Privacy Protection www.privacy.ca.gov January 28, 2009 1	
Slide 2	 2	We use our computers for all kinds of sensitive transactions – banking, stock trading, filing income taxes. We store personal information on our computers – medical records, tax information. Are the computers in our homes as secure as the computers on our desks at work?
Slide 3	 Home computers lack basic security protections.	According to the *2008 National Cyber Security Alliance-Symantec Online Safety Study*, many Americans still fail to use basic Internet security tools. There's a big gap between protections people think they have and what's actually installed on their computers.

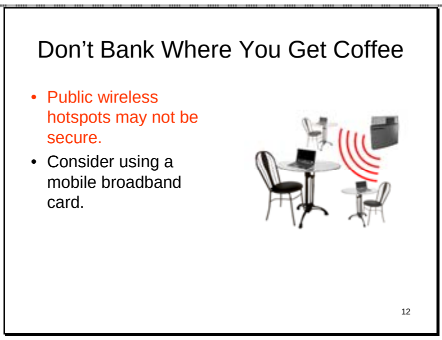
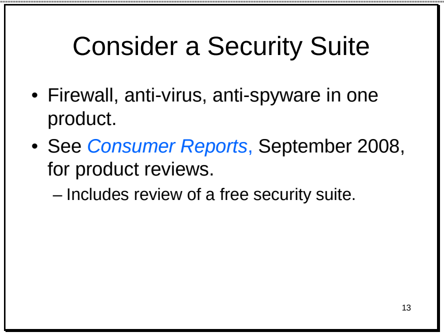
		For example, more than 80% claim to have a firewall installed – yet scanning revealed that only 42% had adequate firewall protections.
Slide 4	 Botnets • 100-150 million PCs in botnets – 20-30% of total PCs in world. • Botnets of zombie computers responsible for 80% of world's spam. 1 Compromise as many devices as possible Bot Bot Bot Bot Bot Command & Control 2 Send commands to bots 3 Execute commands Attacker 4 Source: Jonathan Zittrain, *The Future of the Internet and How to Stop It*	Your computer may be a zombie slave, part of a "botnet", a network of computers that is sending spam or malware on behalf of someone controlling the network remotely - often a criminal enterprise. It is estimated that there are 100-150 million PCs in botnets – 20-30% of PCs in the world. Botnets of zombie computers are responsible for 80% of the world's spam.
Slide 5	 Crime Drives "Badware" • Malware is multiplying. – 1988: 1,738 – 1998: 177,615 – 2008: 1.1 MM+ • Malware is sophisticated. – New version every 2.5 seconds. • Malware is profit-driven. – Targeted, organized crime. 5 Source: Trend Micro Inc.	Viruses and spyware are examples of malicious software, or "malware," that can take over your computer and even steal your personal information. And malware is multiplying on the Internet. Malware is becoming more sophisticated, changing and adapting constantly. It's challenging for the good guys to keep up with. Malware is used by organized criminal enterprises to make

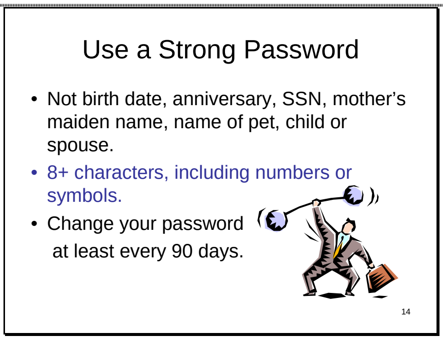
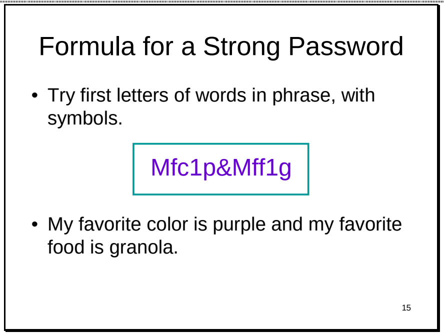
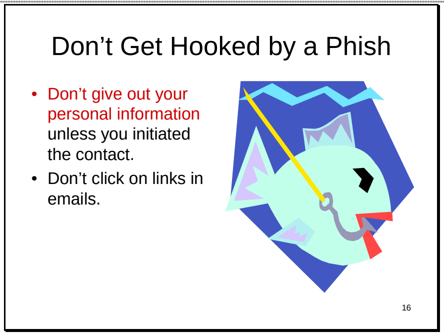
		money. They steal personal information to sell and use. Including targeted attacks on privileged individuals – to get their passwords and access rights.
Slide 6	 Protect Your Computer • Use an Internet firewall. • Keep your operating system and browser up to date. • Install and maintain anti-virus software. • Install and maintain anti-spyware software. 6	By taking 4 basic steps, you can help secure your PC from many malicious attacks. 1. Use an Internet firewall 2. Keep your operating system up to date, preferably by using automatic update feature. 3. Install and maintain anti-virus software. 4. Install and maintain anti-spyware software.
Slide 7	 Use a Firewall • Like a barrier between your computer and the Internet. VPN Client Software Standalone Firewall Internet Firewall Router 7	A firewall creates a barrier between your PC and the Internet – a security checkpoint that information and software must pass through before being allowed to enter your computer. It's your first line of defense, because it helps to make your computer invisible to online attackers and many types of malicious software, such as viruses and worms. Remember, a recent survey found that while **81%** said they had computer firewalls, only **42%** actually had them installed and enabled.

Slide 8	 Keep Your OS Updated Control Panel File Edit View Favorites Tools Help Search Folders Address Control Panel Accessibility Options Add Hardware Add or Remov... Administrative Tools Adobe Gamma Automatic Updates Data Sources (ODBC) Date and Time Display Folder Options Fonts Game Controllers Intel(R) Extrem... Internet Options Java Keyboard Mail Microsoft Mail Postoffice Mouse Network Connections Network Setup Wizard Phone and Modem ... Portable Media Devices Power Options Printers and Faxes QuickTime Regional and Language ... Scanners and Cameras Scheduled Tasks Sounds and Audio Devices Speech Symantec LiveUpdate System Taskbar and Start Menu User Accounts Windows Firewall Windows Media Connect Wireless Network Set... Set up Windows to automatically deliver important updates 8	Regularly update your computer operating system with security updates provided by the manufacturer. If you use a Windows OS, you can protect your PC automatically by using the Windows Automatic Update feature. Once you turn on Windows Automatic Update, you will get new security updates to your computer as soon as they are available. The updates will be installed automatically the next time you turn on your computer.
Slide 9	 Install Anti-Virus Software And keep it updated. 9	A computer virus is a program that can copy itself and infect a computer without permission or knowledge of the user. Anti-virus software helps to protect your computer by scanning every email, application or piece of content that enters your PC. Strong anti-virus programs can detect and destroy thousands of specific viruses before they have a chance to damage your system. Online attackers are constantly creating new viruses.

		To protect your PC from these threats, make sure you never let your anti-virus program expire, and keep the software up to date with the latest updates from the manufacturer.
Slide 10	 Install Anti-Spyware Software Keep it updated too! 10	Spyware is software that is installed surreptitiously on a PC to intercept or take partial control over the computer, without the user's consent. Spyware can drown you in pop-up ads and slow down your computer’s functions. Spyware called keyloggers can even steal your personal information as you type it into your computer. Anti-spyware software can reveal (and let you destroy) any spies already on your system, and help to keep your computer running smoothly and prevent further intrusion. As with your operating system and anti-virus software, it’s essential to keep your anti-spyware software updated.

Slide 11	 Secure Your Wireless Network • Use a wireless router with encryption. • Change the default password & router identifier. • Turn off your wireless network when not in use. To internet Cable modem Wireless router Desktop with PCI wireless adapter Laptop with wireless adapter card 11	If you use a wireless network in your home, be sure to take precautions to secure it against hackers. Encrypting wireless communications is the first step. Choose a wireless router with an encryption feature and turn it on. If your router enables identifier broadcasting, disable it. Note the SSID name so you can connect your computers to the network manually.[1] Be sure to change the default identifier on your router and the pre-set administrative password. Hackers know the defaults. Turn off your computer when you’re not using it. [1] SSID is Service Set Identifier, the name a manufacturer assigns to a wireless network router. The same SSID may be assigned to all hardware of the same type.

Slide 12	 Don't Bank Where You Get Coffee - Public wireless hotspots may not be secure. - Consider using a mobile broadband card. 12	Remember that public “hot spots” may not be secure. It’s safest to avoid accessing or sending sensitive personal information over a public wireless network. You may also consider buying a mobile broadband card that will allow you to connect to the Internet without relying on Wi-Fi hot spots. A mobile broadband card is a device that plugs into your computer, laptop, PDA, or cell phone and uses a cell phone signal to provide high-speed Internet access. They are sold by cell phone companies and require a monthly service plan.
Slide 13	 Consider a Security Suite - Firewall, anti-virus, anti-spyware in one product. - See *Consumer Reports,* September 2008, for product reviews. – Includes review of a free security suite. 13	The independent nonprofit Consumers Union provides product reviews and strategies. See the September 2008 article on ConsumerReports.org, "Get the Most from Security Software," available for free online. (Product ratings are available online to subscribers only.) Or see a copy at your local library. It includes a review of e security software you can download for free to create your own “mini-suite.” .

Slide 14	 Use a Strong Password • Not birth date, anniversary, SSN, mother's maiden name, name of pet, child or spouse. • 8+ characters, including numbers or symbols. • Change your password at least every 90 days. 14	Don't use obvious and easily learned passwords – like mother's maiden name, birthday, pet's name, last 4 digits of your SSN. A strong PW is at least 8 characters in length – with letters and numbers or symbols. Change your PW regularly.
Slide 15	 Formula for a Strong Password • Try first letters of words in phrase, with symbols. Mfc1p&Mff1g • My favorite color is purple and my favorite food is granola. 15	One way to come up with a PW that you can remember but others can't guess is to use the first letters of a phrase or sentence. Then use numbers and/or symbols in place of some letters.
Slide 16	 Don't Get Hooked by a Phish • Don't give out your personal information unless you initiated the contact. • Don't click on links in emails. 16	A "phish" is an email that looks like it's from a bank, a government agency, or some other source whose purpose is to trick you into providing your personal information – your password, Social Security number, financial account number, etc. The safest way to avoid getting hooked is NEVER give out your personal information unless YOU initiated the contact.

		If the email (or it could be a phone call) seems legitimate, look up a phone number for the company or agency in the phone book and call them to verify BEFORE you provide any information. No legitimate company or organization will request personal information in this way today.
Slide 17	For More Information CALIFORNIA OFFICE OF PRIVACY PROTECTION www.privacy.ca.gov 866-785-9663 17	Information available at www.privacy.ca.gov includes the following: Consumer information sheets on computer security (*CIS 12: Protect Your Computer from Viruses, Hackers and Spies*), identity theft and other privacy topics. Best practice recommendations for businesses. California and federal privacy laws and pending state legislation.